IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA *ex rel*. Michael J. Daugherty, Plaintiff and Relator, v. TIVERSA HOLDING CORP., TIVERSA INC., TIVERSA GOVERNMENT INC. and ROBERT BOBACK, Defendants.	)	Civil Action No. 14-CV-4548-DLC

AMENDED COMPLAINT FOR VIOLATIONS OF THE FALSE CLAIMS ACT

Plaintiff Michael J. Daugherty, on his own behalf and on behalf of the United States of America, by and through his undersigned counsel, hereby files his Amended Complaint as permitted by this Court's July 5, 2018 Order (ECF No. 64), showing the Court as follows:

INTRODUCTION

1. *Qui tam* Relator Michael J. Daugherty ("Daugherty" or "Relator"), brings this action on his own behalf and on behalf of the United States of America to recover damages and penalties under the False Claims Act, 31 U.S.C. § 3729 *et seq*., against Defendants Tiversa Holding Corp., Tiversa Government, Inc., and Tiversa Inc. (collectively "Tiversa") and Tiversa's former Chief Executive Officer Robert J. Boback ("Boback").

2. This case arises out of Defendants' conspiracy and scheme to defraud the United States Government by submitting or causing submission of false or fraudulent claims for payment to the United States in the context of government contracts relating to cybersecurity. This includes federal grant funds provided by the Department of Homeland Security ("DHS") for critical

research on cybersecurity and worthless services provided by Tiversa to the Transportation Security Administration ("TSA").

3. Defendants have abused the public trust. Through their intentional fraudulent behavior and schemes, they have fraudulently induced the United States to enter into government-funded contracts for monitoring services supposedly to detect sensitive information inadvertently available on peer-to-peer networks. From the inception of Defendants' pitch for and negotiation of its contract with the TSA, addressed in greater detail herein, through the present, Defendants have attempted to conceal and minimize the extent of their fraudulent misconduct, misstatements and material omissions.

4. Defendants have also materially participated in, aided in, and perpetuated systemic research misconduct and fraud in research funded by a $30 million federal grant. Defendants' knowing and intentional actions in the context of the federally-funded research yielded results that were intentionally and known to be false, fabricated, manipulated and misleading. From the inception of Defendants' participation in a federally-funded research project with Dartmouth College, addressed in greater detail herein, through the present, Defendants have attempted to conceal and minimize the extent of their fraudulent misconduct.

5. Defendants' fraud, false statements, material omissions and lies induced the United States, through the TSA, to expend federal dollars on a contract for cybersecurity services that it would never have entered into had it known the fraudulent activity in which Defendants engaged to falsely create the perceived need for these contract services and had it known that Defendants' services were worthless. Defendants' fraud, false statements, material omissions and lies also substantially damaged the DHS grant process and the United States' national security interests by

diverting scarce government grant funds away from others conducting honest and legitimate cybersecurity security research and through causing the publication of fraudulent research.

6. Under the FCA, Defendants are liable to the United States for the ill-gotten gains and misspent grant funds, as well as other damages and civil penalties.

JURISDICTION AND VENUE

7. This action arises under the United States Civil False Claims Act, 31 U.S.C. § 3729 *et seq*. ("FCA").

8. The Court has subject-matter jurisdiction pursuant to 31 U.S.C. § 3732(a) and 28 U.S.C. § 1331, and has personal jurisdiction over Defendants because one or more of the Defendants resides, transacts business or can be found in this District.

9. Venue in this District is proper under 28 U.S.C. 1391(b) and (c), and 31 U.S.C. 3732(a).

10. The facts and circumstances regarding the fraud on Government entities alleged in this Amended Complaint have not been publicly disclosed in a federal criminal, civil, or administrative hearing in which the Government or its agent is a party; or in a Congressional, Government Accountability Office, or other federal report, hearing, audit, or investigation; or in the news media; or in any other method or manner that would deprive this Court of jurisdiction over this case. In short, the public disclosure bar of the FCA is inapplicable in this action.

11. Relator is an original source of the information upon which this Amended Complaint is based, as that phrase is used in the FCA. He has knowledge that is independent of and materially adds to any publicly disclosed allegations or transactions, and he has disclosed the facts upon which this action is based to the United States prior to the filing of this Amended Complaint.

PARTIES

12. The real party in interest to the claims set forth herein is the United States of America.

13. Daugherty is a resident of Georgia. Daugherty received his undergraduate degree in Economics from the University of Michigan in 1982. Since that time, Daugherty has worked in a variety of roles within the medical profession. In 1996, Daugherty founded a urology health center, ultimately called LabMD, Inc. ("LabMD"), which was a full-service uropathology and microbiology cancer-detection laboratory. Daugherty is the chief executive officer and sole shareholder of LabMD. LabMD was forced to close its normal business operations in 2014 because of financial difficulties caused in substantial part by Defendants' frauds.

14. Defendants Tiversa Holding Corp. and Tiversa Government Inc. are Delaware corporations, each formed on March 29, 2012. Defendant Tiversa Holding Corp.'s predecessor company, Tiversa, Inc., was a Pennsylvania corporation formed on January 15, 2004. It merged into Tiversa Holding Corp. on April 10, 2012. Tiversa's principal place of business is at 606 Liberty Ave., Pittsburgh, Pennsylvania 15222.

15. Defendant Robert J. Boback is a resident of Florida and is a co-founder and the former Chief Executive Officer of Tiversa.

FACTS

The Technology Underpinning Defendant's Fraudulent Scheme

16. To understand Defendants' fraudulent scheme, some background on peer-to-peer (a/k/a "P2P") technology is in order. A peer-to-peer network is created when one computer is communicates with another without going through a separate central server computer. The purpose of most P2P networks is to allow people to search for, identify and share files (*e.g.*, music,

video, pictures, PDFs) stored in certain folders on computers. P2P applications enable one computer to search certain folders in another computer, so long as the other computer is also using the file-sharing application and are within the radius of the search.

17. In P2P networks, folders that make files available for sharing often contain files that no one ever intended to make available to others. Many computer users do not know when the computers they are using are loaded with P2P software. A child, a former computer owner, a former employee or malware may have downloaded the P2P application. In addition, some creators of P2P applications often deceived users into selecting or automatically designating folders used for everyday needs. *See, e.g.,* "Filesharing Programs and "Technological Features to Induce Users to Share," A Report to the United States Patent and Trademark Office from the Office of International Relations, Prepared by Thomas D. Sydnor II, John Knight and Lee A. Hollaar (November 2006).

18. Tiversa, a so-called cybersecurity company, used several technologies to search for and download massive amounts of data from multiple peer-to-peer networks all across the world. Such data included personal, private, confidential, classified and otherwise sensitive information from computers loaded with P2P software. In many situations, Tiversa would improperly and illegally take files directly from the computers of the unsuspecting individual or companies that owned the files with the full knowledge that the owners would have forbidden and prevented Tiversa's theft if they knew that Tiversa was secretly stealing their files.

19. At all times relevant to this Amended Complaint, Tiversa claimed its patented technologies allowed it to conduct 1.8 billion searches on 500 million computers every day.

The Defendants' Scheme

20. Tiversa claimed that it was free to take whatever files it found because, it claimed, all of the files it took were "publicly available." This claim was legally and factually false for many reasons. As an example, by analogy, under 18 U.S.C. § 1708, it is a felony to steal or take any letter, postal card, package, bag or mail from a collection box or other authorized depository of mail matter. Mail deposited in millions of U.S. mailboxes every day is "available" to anyone but is not considered "publicly available" despite the ease with which mail can be taken from many of those boxes. In similar fashion, Tiversa's possession and use of many of the files it took from others violated federal laws including, but not limited to, 18 U.S.C. § 793 (Espionage Act - Unlawful Gathering and Transmitting of Defense Information), 18 U.S.C. § 798 (Espionage Act - Illegal Disclosure of Classified Information), 18 U.S.C. § 1924 (Unlawful Removal and Retention of Classified Information), 18 U.S.C § 1832 (Economic Espionage Act - Theft of Trade Secrets), 18 U.S.C. § 2511 (Interception and Disclosure of Electronic Communications), 18 U.S.C. § 2701 (Unlawful Access to Stored Communications) and 42 U.S.C. § 1320d-6 (Unlawful Possession and Use of Personal Health Information). Further, only Tiversa, with its "patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day" and its cadre of highly experienced professional hackers, would ever have found and taken the vast majority of files it hacked from the computers of unsuspecting users.

21. To conceal their hacking, to avoid prosecution under the statutes mentioned above, to garner widespread publicity and to create a fictional urgency for their services, Defendants falsely claimed that Tiversa found "leaked" files on computers of known bad actors, such as identity thieves and other criminals, and further falsely claimed that the files it hacked were spreading on peer-to-peer networks.

22. Through a well-organized public campaign of deceit, Defendants fostered the aforementioned fictions for years. In one example, Boback testified before the House Subcommittee on Commerce, Trade and Consumer Protection on May 5, 2009 that, "In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One [Marine One is the call sign used to identify any helicopter used by the Marine Corps to transport the President of the United States]. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran." Tiversa received extensive nationwide publicity for this alleged find. Investigations and revelations from a whistleblower later established that the information was not "apparently downloaded" by anyone in Iran. Instead, Boback instructed an employee to find an IP address in Iran that could be used to perpetuate that lie. The employee did identify such an address, and Boback proceeded to twice falsely testify before Congress that Marine One's information was found there. In an unsuccessful attempt to avoid a revelation of the truth, Tiversa later hired as its Director of Government Services, the NCIS investigator who was investigating Defendants' Marine One story. *See* pp. 17 and 18 of Exhibit A attached hereto.

23. Defendants made millions of dollars by monetizing the files Tiversa took by selling monitoring and remediation services to fix the fictitious problems created by Tiversa. Using the very files Tiversa had improperly stolen from its victims, Defendants would falsely represent to Tiversa's putative customers that the victim of its thefts had a security breach of unknown origin or scope and needed Tiversa's services to identify and remedy the breach. Tiversa and Boback knew that the representations that they were making to the victim clients were intentionally false, and they knowingly and intentionally falsified and aggrandized the source, scope, and severity of

the alleged breach for the sole purpose of selling their cybersecurity services to the victim customer. This was a classic protection racket, updated for the digital age.

Defendants' Scheme Exposed

24. Relator's company, LabMD, was one of many victims of Tiversa's fraudulent scheme. In May 2008, Boback contacted LabMD to inform it that Tiversa had obtained a copy of a LabMD file, allegedly on a P2P network, and that the file was allegedly spreading on peer-to-peer networks. This particular file was a 1,718-page PDF document containing protected personal information on approximately 9,300 patients (the "1718 File"). In truth, Tiversa had accessed and downloaded the 1718 File directly from a LabMD billing computer in Atlanta, Georgia, on February 25, 2008. Tiversa never found the 1718 File anywhere other than on a LabMD computer, and its allegations that the file was spreading on other P2P networks were entirely fabricated.

25. After LabMD heard from Boback, it immediately identified that an employee's computer had a P2P application installed on it. LabMD removed both the software and the file from the computer right away.

26. Relator asked Boback to provide details regarding the file and how Defendants had come to find it but Boback refused to provide any meaningful details unless LabMD signed a contract with Tiversa.

27. All subsequent attempts by Relator to glean additional information about how Tiversa accessed the LabMD file were met with essentially the same response: "we won't tell you anything now, but we can help you if you hire us." Defendants went so far as to threaten Relator that if LabMD refused to pay, Defendants would report LabMD to the Federal Trade Commission ("FTC"), an agency that was working with Tiversa to prosecute companies for allegedly not keeping confidential consumer information secure.

28. Defendants followed through on their threat by reporting LabMD to the FTC along with scores of other companies that also refused to pay Tiversa for its "services."

29. Defendants falsely told the FTC that it "found" LabMD's file because LabMD had made it "publicly available" on the internet, that LabMD's file was spreading to other computers on the internet and that identity thieves and other criminals had already gotten copies of and were distributing the 1718 File to others. At the time that Tiversa and Boback made these statements to the FTC, they knew that the statements were substantially and materially false.

30. The FTC investigated LabMD for three and a half years, all due to Tiversa's theft of LabMD's file and incessant lies about the 1718 File's origin and whereabouts.

31. On August 28, 2013, the FTC filed an administrative enforcement action against LabMD (the "Enforcement Action"), relying almost exclusively on the file Tiversa had stolen from LabMD and the lies Tiversa was telling about that file.

32. On April 2, 2014, Richard Wallace, a former Tiversa employee, blew the whistle on Tiversa and its illegal scheme by exposing many of Defendants' crimes and lies to Relator.

33. On November 14, 2014, the U.S. Attorney General issued Wallace a grant of immunity pursuant to 18 U.S.C. § 6002. Pursuant to that grant of immunity, Wallace testified under oath in the Enforcement Action on May 5, 2015, where he disclosed the following:

- On February 25, 2008, Tiversa located the 1718 File on a LabMD computer near Atlanta, Georgia.
- Tiversa never found the 1718 File anywhere other than on a LabMD computer.
- At Boback's direction, Tiversa employees would manipulate the data in Tiversa's data repositories to make it appear that prospective customers' files had spread to other locations on the peer-to-peer networks.
- Wallace testified about a list of names and other information on approximately 89 companies that Tiversa created to give to the FTC in response to a civil investigative demand the FTC would serve on The Privacy Institute, a sham corporation created by

Tiversa so that it could provide selective documents to the FTC. According to Tiversa, all of the companies on this list had experienced data breaches.

- Boback told Wallace to include LabMD on the list in retaliation for LabMD not hiring Tiversa.

- Shortly before Boback's deposition in the Enforcement Action, Boback told Wallace to change the data in Tiversa's data store to make sure that the 1718 File did not appear to have come from the Atlanta area.

- Boback directed Wallace "that under no circumstances can the insurance aging file originate from a Georgia IP address or an Atlanta area IP address. And in addition to that, [Boback] told [Wallace] to find an individual in San Diego [a known identity thief] to include with this list."

34. Wallace's testimony was so convincing that the FTC ultimately withdrew *all reliance* upon Tiversa's false testimony and fabricated evidence and the Commission later acknowledged, "[W]e agree that Mr. Boback's assertion that Tiversa had gathered evidence showing that the 1718 file had spread to multiple Internet locations by means of LimeWire was false[.]" *See In the Matter of LabMD, Inc*., 2016 FTC LEXIS 128, *91 (F.T.C. July 28, 2016).

35. Wallace's revelations also resulted in a parallel congressional investigation which culminated in a 99-page report addressing Tiversa's schemes and its collusion with the FTC. *See* STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 113TH CONG., TIVERSA, INC.:WHITE KNIGHT OR HIGH-TECH PROTECTION RACKET (2015) (the "OGR Report"). A true and correct copy of the OGR Report is attached hereto as Exhibit A and is incorporated herein by reference.

36. Wallace's revelations are also discussed in Chief Administrative Law Judge Michael D. Chappell's ruling in favor of LabMD and against the FTC in the Enforcement Action. *See* Initial Decision, *In re LabMD*, No. 9357 (Nov. 13, 2015), vacated by Opinion of the Commission, (July 29, 2016), stayed sub nom., *LabMD, Inc. v. FTC*, No. 16-16270-D (11th Cir. Nov. 10, 2016). A true and correct copy of the Initial Decision is attached hereto as Exhibit B and

is incorporated by reference herein. On June 6, 2018, the Eleventh Circuit Court of Appeals vacated the Commission's decision to vacate Chief Administrative Law Judge Michael D. Chappell's Initial Decision. *See LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018).

37. On March 1, 2016, the Federal Bureau of Investigation and the Department of Justice (from the Manassas, VA and Washington, D.C. offices of those organizations) raided Tiversa's headquarters in Pittsburgh, Pennsylvania due to allegedly false statements Boback made to the FTC and Congress regarding Tiversa's theft of files, including the 1718 File, and Tiversa's misrepresentations and fabricated evidence regarding the source and origin of those files.

Defendants' False Statements, False Claims and Frauds

1. Department of Homeland Security and Transportation Security Administration

38. In the first half of 2011, Tiversa found sensitive information related to aircraft computers on a computer of a TSA employee in Denver, Colorado. Boback then instructed Wallace to create a report with fake IP addresses to make it appear that the sensitive information was spreading through peer-to-peer networks.

39. In late spring or summer of 2011, Boback met with representatives of the Department of Homeland Security ("DHS")[1] and the Transportation Security Administration ("TSA")[2] at a DHS office in in Arlington, VA. On information and belief, one of the individuals with whom Boback met was Greg Maier, Chief Information Technology Security Operations for DHS.

40. Boback showed Maier and others Wallace's fabricated report and falsely informed them that sensitive search procedures for aircraft computers had been found on computers in

[1] DHS is department of the United States and is funded by the federal government.
[2] TSA is an agency of the United States and is funded by the federal government.

foreign countries (possibly including Colombia, Yemen and/or Kenya). In truth, Tiversa did not find the sensitive information on any computer other than the aforementioned computer of the TSA employee in Denver. Boback and Tiversa knew that fact and knew the representations that the sensitive information was found on other computers were fabricated and false.

41. Boback and Tiversa lawyer Eric Kline later traveled to Arlington to negotiate a Firm Fixed Price Definitive Contract, PIID number HSTS0311CCIO554, which was signed on August 3, 2011 (the "Definitive Contract").

42. A May 17, 2011 Synopsis described the anticipated Definitive Contract as follows:

> The Transportation Security Administration (TSA) intends to contract using other than full and open competition for the following: Peer to Peer Intelligence Service which is a monitoring service to detect sensitive information inadvertently or intentionally disclosed or posted on a network. Also, Peer to Peer provides forensic services when data is discovered. Accordingly, the TSA intends to award a contract to TIVERSA INC, 144 EMERYVILLE DR STE 300 CRANBERRY TOWNSHIP PA 16066-5015 USA. This contract will address the requirements of the TSA Office of Information Technology/Information Assurance and Cyber Security Division (IAD), and the Office of Acquisition for Peer to Peer Intelligence Service. The proposed contract action is to procure a Peer to Peer monitoring service that will detect sensitive information inadvertently disclosed on a network and provide, at the same time, file takedown services to remediate sensitive files disclosures. The Government intends to solicit and negotiate with only the above designated source under the authority of FAR 6.302-1.

43. The DHS was the award agency and TSA was the award bureau. Under the Definitive Contract, Tiversa, Inc. was paid $324,000 to provide intelligence monitoring and detection services from August 3, 2011 through August 2, 2012, for the purpose of monitoring and locating exposed files such as sensitive type files, determining file sources and help in remediation and/or risk mitigation. Documentation related to this contract is attached hereto as Exhibit C and is incorporated by reference herein.

44. Upon information and belief, Tiversa falsely reported to TSA that it found TSA files of interest at various IP address computers. In truth, Tiversa followed its fraudulent *modus*

operandi and included fake IP addresses to make it appear that the sensitive information was spreading through peer-to-peer networks and to foster the need for Tiversa's continued services when it knew that information was false.

45. The Definitive Contract included an option for an extension ("Extension"). On July 2, 2012, the Definitive Contract was extended until August 2, 2013. Again, DHS was the award agency and the TSA was the award bureau. Under the Extension, the government paid Tiversa, Inc. $324,000 for the aforedescribed services from August 3, 2012 through August 2, 2013. Documentation related to the Extension is attached hereto as Exhibit D and is incorporated by reference herein.

46. Tiversa and Boback's false report, false representations, material omissions and lies were misleading, and they fraudulently induced the United States (through DHS and TSA) to enter into the original Definitive Contract and the Extension with Tiversa. Had DHS and/or TSA known the true facts -- that Defendants had instructed Tiversa's employee, Wallace, to generate a false report regarding the scope and severity of the Denver TSA breach for the express purpose of deceiving the Government and causing it to enter into a contract with Tiversa – the United States would not have entered into the Definitive Contract or the Extension.

47. Had the Government known of Boback and Tiversa's fraudulent conduct, it is likely that it would have exercised its right to debar Tiversa and its affiliates from government contracting eligibility.

48. The Definitive Contract and the Extension were procured by Defendants' lies and fraud, rendering all the payments of federal monies thereunder fraudulent.

49. This type of fraud in the inducement and alleged fraud in the performance of Government contracts is the type of fraud that the United States actively prosecutes and that has

served as the basis for numerous criminal and civil enforcement actions by the United States, including in *qui tam* cases under the FCA. Some examples of those actions are set forth below.

50. Tiversa and Boback's fraud in the inducement of the Definitive Contract and the Extension and, on information and belief, in the performance of the TSA contracts, was material to the United States' decision to contract with and pay money to Tiversa under the Definitive Contract.

2. Department of Homeland Security's $30 Million Grant to Dartmouth College

51. On September 25, 2006, DHS awarded a grant, Award Number 2006-CS-001-000001, to Dartmouth College ("Dartmouth") for the administration and completion of an approved Homeland Security program/project within two and a half years from September 30, 2006 through March 30, 2009, unless extensions were approved contingent on acceptable performance of the projects by the DHS, acceptance and approval of each non-competing continuation application by the DHS and available annual DHS appropriations. The title of the award was Cyber Security Collaboration and Information Sharing. A true and correct copy of the Dartmouth Grant Award Terms and Conditions for Award Number 2006-CS-001-000001 (the "September 25, 2006 Grant") is attached hereto as Exhibit E (with personal information redacted) and is incorporated herein by reference.

52. As shown below, the total funding DHS gave to Dartmouth for the Cyber Security Collaboration and Information Sharing project approximated $30 million.

53. All of the DHS grants identified herein were paid with federal funds.

54. Dartmouth made claims for federal funds pursuant to the grants identified herein.

55. DHS paid Dartmouth under the grants identified herein based upon Dartmouth's claims to them.

56. DHS based its decision to pay Dartmouth the federal funds identified herein in material part on the accuracy and veracity of the progress reports Dartmouth was required to submit under the terms and conditions of the grants.

57. Professor M. Eric Johnson, formerly the Director for the Center for Digital Strategies in the Tuck School of Business at Dartmouth College, participated in the proposals for funding and implementation of Dartmouth's work on the Cyber Security Collaboration and Information Sharing project.

58. Johnson was at all times related hereto an employee of Dartmouth who was acting within the scope of his employment.

59. All of Johnson's actions, omissions and intentions alleged herein are attributable to Dartmouth.

60. Johnson engaged Tiversa to partner with him in implementing Dartmouth's work on the Cyber Security Collaboration and Information Sharing project.

61. Johnson had engaged Tiversa to partner with him on other research projects starting as early as September 2005.

62. The September 25, 2006 Grant obligated Dartmouth to provide Quarterly Performance Reports which were required to compare actual accomplishments to the approved project objectives.

63. The September 25, 2006 Grant included the contract provisions listed under OMB Circular A-110 (which establishes uniform administrative requirements for Federal grants and agreements awarded to institutions of higher education, hospitals, and other non-profit organizations.). A true and correct copy of OMB Circular A-110 is attached hereto as Exhibit F and is incorporated herein by reference.

64. Under Section 61 of the OMB Circular A-110, an award may be terminated by the Federal awarding agency, if a recipient materially fails to comply with the terms and conditions of an award.

65. Under Section 62 of the OMB Circular A-110, if a recipient materially fails to comply with the terms and conditions of an award, whether stated in a Federal statute, regulation, assurance, application, or notice of award, the Federal awarding agency may take one or more of the following actions, as appropriate in the circumstances (1) temporarily withhold cash payments pending correction of the deficiency by the recipient or more severe enforcement action by the Federal awarding agency; disallow (that is, deny both use of funds and any applicable matching credit for) all or part of the cost of the activity or action not in compliance; (2) wholly or partly suspend or terminate the current award; (3) withhold further awards for the project or program and (4) take other remedies that may be legally available

66. Under Section 72 of the OMB Circular A-110, the closeout of an award does not affect the right of the Federal awarding agency to disallow costs and recover funds on the basis of a later audit or other review and the obligation of the recipient to return any funds due as a result of later refunds, corrections, or other transactions.

67. Under Section 73 of the OMB Circular A-110, any funds paid to a recipient in excess of the amount to which the recipient is finally determined to be entitled under the terms and conditions of the award constitute a debt to the Federal Government.

68. By law, all applicable statutes, regulations, and rules applicable to DHS grants are incorporated into each of the Dartmouth grants identified herein and are required to be followed.

69. The initial budget period for the Dartmouth Grant was for six months from September 30, 2006 through March 30, 2007, with an approved budget of $930,000, as requested by Dartmouth.

70. On April 3, 2007, DHS awarded a grant, Award Number 2006-CS-001-000002, to Dartmouth College, in furtherance of the Cyber Security Collaboration and Information Sharing project. The award requested by Dartmouth was in the amount of $11,730,00 for the second budget period. Dartmouth was obligated to perform the work described in the Program Narrative Statement as submitted in the Grant Application dated February 22, 2007. A true and correct copy of the Dartmouth Grant Award Terms and Conditions for Award Number 2006-CS-001-000002 (the "April 3, 2007 Grant") is attached hereto as Exhibit G (with personal information redacted) and incorporated herein by reference.

71. The second budget period was for six months from April 1, 2007 through March 31, 2008.

72. On June 18, 2007, DHS amended Award Number 2006-CS-001-000002 to provide an additional $3.3 million in funding as requested by Dartmouth (the "June 18, 2007 Grant") Amendment No. 2 to Award Number 2006-CS-001-000002 is attached hereto as Exhibit H (with personal information redacted) and is incorporated herein by reference.

73. On February 4, 2008, Dartmouth represented to DHS that its "overarching goal is to spend these government funds responsibly and ensure projects are carried out in a legal and ethical manner." Exhibit I hereto is a true and correct copy of the February 4, 2008 letter, which is incorporated herein by reference.

74. On May 20, 2008, DHS awarded a grant, Award Number 2006-CS-001-000003, to Dartmouth College, in furtherance of the Cyber Security Collaboration and Information Sharing

project. This award, requested by Dartmouth, was in the amount of $8,340,000 for the third budget period. Dartmouth was obligated to perform the work described in the Program Narrative Statement as submitted in the Grant Application dated January 28, 2008. A true and correct copy of the Dartmouth Grant Award Terms and Conditions for Award Number 2006-CS-001-000003 (the "May 20, 2008 Grant") is attached hereto as Exhibit J (with personal information redacted) and incorporated herein by reference.

75. The third budget period was for six months from August 1, 2008 through July 31, 2009, and was later extended until July 31, 2011.

76. On or about February 22, 2009, M. Eric Johnson of the Center for Digital Strategies at the Tuck School of Business at Dartmouth College published "Data Hemorrhages in the Health-Care Sector," in a publication entitled "Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers. (the "Johnson's Paper") A true and correct copy of the Johnson Paper is attached hereto as Exhibit K and is incorporated by reference herein.

77. Dartmouth anticipated that Johnson would author the Johnson Paper when it submitted its proposal for the Dartmouth Grant.

78. The research detailed in the Johnson Paper was supported by the Dartmouth Grant. The federally-funded Johnson Paper analyzed the consequences of files leaked over internet file-sharing networks.

79. The Johnson's work and the Johnson Paper and its findings received widespread press. Exhibit L hereto is a true and correct copy of an article from the March 2, 2009 edition of WIRED magazine titled, "Academic Claims to Find Sensitive Medical Info Exposed on Peer-to-

Peer Networks." Exhibit M hereto is a true and correct copy of an article January 30, 2009 edition of Computerworld magazine.

80. Johnson explains in a footnote on the first page of the Johnson Paper, "Experiments described in this paper were conducted in collaboration with Tiversa who has developed a patent-pending technology that, in real-time, monitors global P2P file sharing networks." Tiversa was motivated to work with Johnson on the Cyber Security Collaboration and Information Sharing project so long as it received credit and publicity. Johnson understood and agreed to this, as shown in the email referenced below where he promises to coordinate with Tiversa on the release of the Johnson Paper.

81. Johnson further stated in the footnote on the first page of the Johnson Paper, "This research was partially supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P)."

82. In a section of the Johnson Paper titled "Research Methods and Analysis," Johnson described the search protocol for his research. Johnson stated, "To collect a sample of leaked data, we initially focused on Fortune Magazine's list of the top ten publically [sic] traded health-care firms (Fortune Magazine (Useem 2007))." Johnson then stated his team developed a "digital footprint" (key terms) for each health care institution and "with the help of Tiversa Inc., we searched P2P networks using our digital signature over a 2-week period (in January, 2008) and randomly gathered a sample of shared files related to health care and these institutions."

83. Johnson, based upon representations made to him by Defendants, claimed to have located LabMD's 1718 file using this methodology, and Johnson relied heavily on the 1718 File, its contents and how it was found in his research paper. These representations regarding the way

the 1718 File was located were false and known to be false by Defendants. Tiversa and Johnson did not find the 1718 File with the search protocols described by Johnson. Instead, as Relator was told by the whistleblower in February 2017, Tiversa used proprietary law enforcement software developed and owned by the U.S. Government to search for, access and steal the 1718 File. It did not use its "patent-pending technology that, in real-time, monitors global P2P file sharing networks," as represented in the Johnson Paper.

84. In the "second stage of our analysis," Johnson explained that using information from the first search discussed above, his team "examined shared files on hosts where we had found other dangerous data" and "over the next six months, we periodically examined hosts that appeared promising for shared files." Johnson further explained in his Paper:

> Using this approach, we uncovered far more disturbing files. For a medical testing laboratory, we found a 1,718-page document containing patient Social Security numbers, insurance information, and treatment codes for thousands of patients. Figure 4 shows a redacted excerpt of just a single page of the insurance aging report containing patient name [sic], Social Security number, date of birth, insurer, group number and identification number. All together [sic], almost 9,000 patient identities were exposed in a single file, easily downloaded from a P2P network.

85. The following, Figure 4 from Johnson's Paper, is a portion of the 1718 File that was stolen by Tiversa and fraudulently misrepresented in the Johnson Paper:

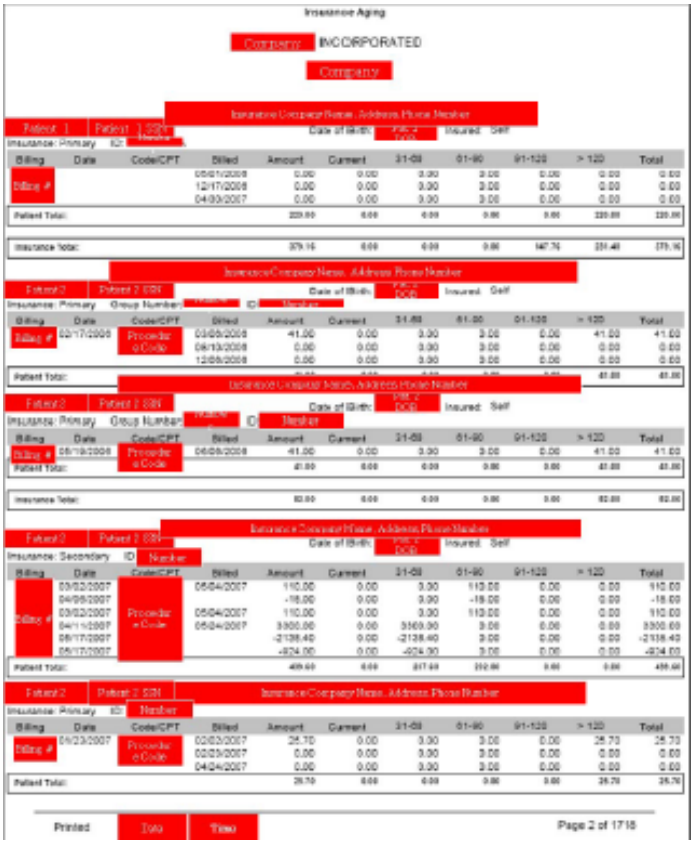

Fig. 4. Excerpt of an insurance againg [sic] report. It contains 1718 pages of patient names, social security numbers, and dates of birth, insurers, group numbers, and identification numbers (exposing nearly 9000 patients). Personally Identifiable Information has been redacted to protect the identities of the disclosers and patients.

86. Johnson was subpoenaed to testify and produce certain documents at a deposition taken of him on February 18, 2014, in the Enforcement Action against LabMD. Documents produced by Johnson prove that he made false statements and false representations to the DHS and others regarding his search protocols and the 1718 File.

87. As shown in an email attached hereto as Exhibit N, which is incorporated by reference herein, Johnson said the following in an email to Tiversa employee Chris Gormley on

April 29, 2008, several months after the two-week first stage analysis was completed in January 2008:

> We are coming well on the medical files – finished going through all the files. We are working on the report right now. We turned up some interesting stuff – not as rich as the banks, but I guess that could be expected. **Any chance you could share a couple other of your recent medical finds that we could use to spice up the report? You told me about the one database your [sic] found that could really boost the impact of the report.** Certainly will coordinate with you on the report and release. I forgot to ask- did you guys also grab searches related to our digital signature?

(Emphasis added).

88. In response to Johnson's request, Tiversa sent Johnson the 1718 File. Tiversa knew that the 1718 File was not found pursuant to Dartmouth's search protocols.

89. Tiversa was well aware of Johnson's search protocols and falsely stated that they followed it in a May 2009 Press Release where Tiversa actively marketed the DHS-study in the promotion of its own services. A true and correct copy of Tiversa's May 28, 2009 Press Release is attached hereto as Exhibit O and is incorporated by reference herein. Upon information and belief, it used its role in the Dartmouth grant's Johnson research to solicit and receive additional government contracts.

90. Johnson knew that the 1718 File was not found in accordance with Dartmouth's search protocols and knew that a representation that the 1718 File was found pursuant to the search protocols would be false. Johnson later made the false representation in order to "spice up" his Paper, to impress DHS, to establish his worth to the Cyber Security Collaboration and Information Sharing project and to ensure that Dartmouth continue to receive funding from DHS under the grants identified herein.

91. As established in the testimony of the whistleblower in the Enforcement Action and as admitted by the FTC, Tiversa hacked the 1718 directly from a LabMD computer on February

25, 2008. The 1718 File was never found on any other computer. Other than employees at LabMD, Tiversa, Dartmouth and Johnson were the only ones who ever took, possessed, saw and/or used the 1718 File.

92. Because the 1718 File was not found in the "second stage of the analysis" and did not come from "shared files on hosts where [Dartmouth and Tiversa] had found other dangerous data," those representations by Johnson were false.

93. Johnson also falsely represented in his Paper that the 1718 File was "easily downloaded from a P2P network." From the date the 1718 File was placed on a LabMD computer with LimeWire (approximately August 1, 2007) until the date Tiversa hacked the file from LabMD's computer (on February 28, 2008), Tiversa had performed 374 *billion* searches[3] without locating the 1718 File.

94. Johnson's representation that Tiversa used its "patent-pending technology that, in real-time, monitors global P2P file sharing networks" was also false. As noted above, Tiversa used proprietary FBI surveillance software developed and owned by the United States Government to search for, access and download the 1718 File.

95. Regardless of how Tiversa obtained the 1718 File, it was a crime for it to possess and use the 1718 File. Tiversa's possession and use of the 1718 File violated 42 U.S.C. § 1320d-6, which provides:

(a) Offense

A person who knowingly and in violation of this part—

(1) uses or causes to be used a unique health identifier;

[3] August 1, 2007 to February 25, 2008 = 208 days x 1.8 billion daily searches = 374 billion searches.

> (2) obtains individually identifiable health information relating to an individual; or
>
> (3) discloses individually identifiable health information to another person,
> shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d–9 (b)(3) of this title) and the individual obtained or disclosed such information without authorization.
>
> (b) Penalties
>
> A person described in subsection (a) of this section shall—
>
> (1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
>
> (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
>
> (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

96. LabMD is a covered entity under HIPAA.

97. Under 42 U.S.C. § 1320d-6, it was also a crime for Dartmouth and Johnson to possess and use the 1718 File.

98. At no time did Dartmouth disclose to DHS Tiversa's violation of 42 U.S.C. § 1320d-6.

99. At no time did Dartmouth disclose to DHS Dartmouth and Johnson's violations of 42 U.S.C. § 1320d-6.

100. Research misconduct is critically important and material to the U.S. Government. *See* "Federal Policy on Research Misconduct, Office of Science and Technology Policy," Federal Register (December 6, 2000), Volume 65, Number 235, Pages 76260-76264. A true and correct copy of this policy is attached hereto as Exhibit P and is incorporated by reference herein. This policy, which was implemented on December 6, 2001, applies to federally funded research and

proposals submitted to Federal agencies for research funding, including, without limitation, to Dartmouth's proposal for the Dartmouth Grant, Dartmouth's quarterly progress reports, Dartmouth's Project Narratives and Dartmouth's requests for additional and supplemental funding of the Dartmouth Grant.

101. Research misconduct is important and material to DHS, so much so that DHS has issued Management Directive No. 10500 where DHS states it will take appropriate action against individuals or institutions upon a finding that research misconduct has occurred. DHS defines "research misconduct" to include fabrication ("Making up data or results and recording or reporting them") and falsification ("Manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record."). A true and correct copy of Management Directive No. 10500 is attached hereto as Exhibit Q and is incorporated by reference herein.

102. The Johnson Paper includes fabrication and falsification of facts, research methods and search protocols.

103. Defendants, Johnson and Dartmouth conspired to violate the FCA.

104. Dartmouth never disclosed to DHS that Tiversa had, in fact, obtained the 1718 File outside of its search protocols and that it nevertheless intended to rely on and represent that the 1718 File was found within its search protocols in order to "spice up" the Johnson Paper.

105. Dartmouth never disclosed to DHS that Tiversa did not use its "patent-pending technology" to obtain the 1718 File.

106. Dartmouth never disclosed to DHS that Johnson planned to and did falsely represent in his Paper that the 1718 File was "easily downloaded from a P2P network."

107. On August 10, 2009, DHS awarded Dartmouth, pursuant to Dartmouth's request, supplemental funding of $2,250,000 pursuant to Award Number 2006-CS-001-000003. A true and correct copy of the Dartmouth Grant Award Terms and Conditions for Amendment No. 3 to Award Number 2006-CS-001-000003 (the "August 10, 2009 Supplement") is attached hereto as Exhibit R (with personal information redacted) and incorporated herein by reference.

108. The third budget period from August 1, 2008 through July 31, 2011, and was later extended until July 31, 2012.

109. On August 6, 2010, DHS awarded Dartmouth, pursuant to Dartmouth's request, supplemental funding of $2,250,000 pursuant to Award Number 2006-CS-001-000003. A true and correct copy of the Dartmouth Grant Award Terms and Conditions for Amendment No. 5 to Award Number 2006-CS-001-000003 (the "August 6, 2010 Supplement") is attached hereto as Exhibit S (with personal information redacted) and incorporated herein by reference.

110. The third budget period from August 1, 2008 through July 31, 2012, and was later extended until July 31, 2013.

111. On September 14, 2011, DHS awarded Dartmouth, pursuant to Dartmouth's request, supplemental funding of $850,000 pursuant to Award Number 2006-CS-001-000003. A true and correct copy of the Dartmouth Grant Award Terms and Conditions for Amendment No. 7 to Award Number 2006-CS-001-000003 (the "September 14, 2011 Supplement") is attached hereto as Exhibit T (with personal information redacted) and incorporated herein by reference.

112. The third budget period from August 1, 2008 through July 31, 2013, and was later extended until July 31, 2014.

113. The total of the aforedescribed grants to Dartmouth was $29,650,000.

114. Recipients of DHS grants are required to submit timely, complete and accurate quarterly progress reports to DHS. For the period January 1 – March 31, 2009, Dartmouth made a required quarterly report to DHS on Initiative 5: Business Rationale for Cyber Security, which was one of the projects funded by the 2006 Award. In that report, Dartmouth touts the Johnson Paper as evidence of its performance under the grants. Dartmouth never disclosed in this report to DHS in this or any other quarterly progress report that it violated 42 U.S.C. § 1320d-6 by virtue of its possession and use of the 1718 File; that Tiversa obtained the 1718 File illegally and outside of Dartmouth's research parameters; that the 1718 File was never found within Dartmouth's search protocols and that the 1718 File was not "easily downloaded from a P2P network."

115. At no time when it requested payment pursuant to the DHS grants identified herein did Dartmouth disclose its failure to comply with (1) the material terms of the DHS grants; (2) the terms of OMB Circular A-110; (3) its obligation to carry out projects in a legal and ethical manner; (4) its obligation to comply with DHS Management Directive No. 10500; or (5) its obligations under the Federal Policy on Research Misconduct, Office of Science and Technology Policy. Nor did Dartmouth disclose that the research results in the Johnson Paper were false and/or fabricated. These failures to disclose made Dartmouth representations regarding its progress under the grants and its compliance with the terms and conditions of the grants materially misleading.

116. Johnson's research parameters and search protocols went to the heart of the research he was performing and the integrity of his results. By providing the 1718 File, a file that Boback and Tiversa knew that they obtained by illegal hacking with the use of proprietary FBI surveillance software, as opposed to by peer-to-peer software that Johnson was studying and writing about for DHS, Tiversa and Boback irreparably tainted Johnson's research and the integrity of its conclusions. The fact that Johnson relied so heavily on the 1718 File in arriving at his

conclusions is strong evidence that Tiversa's and Boback's fraud and misrepresentations were material and went to the heart of this federally funded research. Because the 1718 File was not and would never have been obtained through the methodology that Johnson's research required to be followed, Tiversa's and Boback's provision of this file and Johnson's use of this file as the centerpiece of his written research results and conclusions rendered Johnson's research and project false, fabricated and ultimately of no value to the Government.

117. Dartmouth's quarterly report for the period January 1 – March 31, 2009 was neither accurate nor complete due to Tiversa's intentional misrepresentations and omissions.

118. Misconduct in scientific research includes intentional, knowing or reckless fabrication, falsification, plagiarism and other practices that seriously deviate from those that are commonly accepted within the scientific community for proposing, conducting or reporting research. Based upon the facts set forth herein, Johnson and Dartmouth, aided and abetted by Defendants, committed actionable misconduct in the context of a federal DHS grant.

119. In total, the funding for the full DHS grant was $29,650,000. The funding for the DHS grants after Johnson's email to Tiversa requesting additional information to "spice up" his report was $13,690,000.

120. If DHS had known that the Johnson Paper, which was funded by its grants, was false and that its results were fabricated, it would have, at a minimum, demanded that the portion of the grants used for this false paper whose fabricated results rendered it useless be refunded and would have refused all or portion of additional funding requests related to the Cyber Security Collaboration and Information Sharing project. Additionally, because the Government gets no benefit from federally funded projects that are not performed in conformance with the rules and parameters of the grants themselves, and because Johnson's research methodology went to the

heart or core of the research he was performing and the integrity of his results, the United States, on information and belief, was authorized to and would have pulled some or all the funding for some or all of the grants identified herein. *See, e.g., United States ex rel. Feldman v. Van Gorp*, 697 F. 3d 78, 88 (2nd Cit. 2012) (where Government has provided federal grant funds for a specified good or service only to have defendant substitute a non-conforming good or service a court may find FCA liability and calculate the damages to be the full amount of the grant payments after the material false statements were made).

Scienter

121. Throughout the Amended Complaint, Plaintiffs have demonstrated how and why Boback's and Tiversa's false statements, fabricated reports and data, fraud, lies, and critical omissions that resulted in false claims and false statements being presented to the federal government for payment were knowingly and intentionally made or omitted. All those allegations, the reasonable inferences therefrom, and all facts and statements in the attached exhibits relating to knowledge and intent are incorporated as though fully set forth herein.

122. Tiversa and Boback knew that the misrepresentations and false reports that it presented to the TSA and the material omissions it kept from the TSA to secure its contract with the TSA as described herein were knowingly and intentionally false, fraudulent and faked.

123. Tiversa and Boback intentionally and knowingly lied to TSA and TSA representatives for the express purpose of causing it to enter into and to renew its contract with Tiversa.

124. Tiversa's and Boback's false representations, reports, lies, and material omissions to TSA had a natural tendency to influence and were capable of influencing TSA's decision to

enter into the contract, to renew the contract and to pay Tiversa its submitted claims under the contract.

125. Tiversa and Boback knew that Tiversa's violation of Johnson's research parameters and search protocols and their false statements/representations would render Johnson's research results false, fabricated and worthless.

126. Tiversa and Boback knew that their statements/representations regarding the source of the LabMD 1718 File were false because they knew the true manner in which they had actually obtained the 1718 File. Tiversa also knew that these false statements/representations regarding how and where it found the 1718 File (and potentially other files it supplied to Johnson) rendered Johnson's and Dartmouth's federally-funded research false, fabricated and/or worthless.

127. Tiversa knew that Johnson's study through Dartmouth was federally funded.

128. Tiversa knew that its false statements and fabricated research results would result in false claims being made to the Government.

129. Boback's and Tiversa's false statements, false documents and lies made in connection with the TSA contract and the DHS grants to Dartmouth were made knowingly and intentionally, as alleged herein.

130. Boback and Johnson knew that compliance with the terms of the DHS grants for the Dartmouth study were material to the United States. According to Tiversa, they routinely entered into contracts with the United States, and they are therefore familiar with the process and importance of compliance therewith.

131. Johnson knew or was at least recklessly indifferent to the fact that Tiversa obtained the 1718 File (and potentially other files supplied to him) by methods and means outside of and in violation of his stated research parameters and search protocols. Johnson's email to Tiversa asking

it for material to help "spice up" his research report demonstrates that the results of his actual research within parameters was insufficiently interesting.

Materiality

132. Throughout the Amended Complaint, Plaintiffs have demonstrated how and why Boback's and Tiversa's false statements, fabricated reports and data, fraud, lies, and critical omissions resulted in false claims and false statements being presented to the federal government for payment and how Defendants acts and omissions were material to both DHS's decision to pay Dartmouth, Johnson, and ultimately Tiversa with federal funds from the DHS grants and to TSA's decision to pay Tiversa pursuant to its contract for so-called cybersecurity services. All those allegations and the reasonable inferences therefrom are incorporated as though fully set forth herein.

133. Had the Government known that Tiversa fraudulently induced it into believing that there was a need for Tiversa's cybersecurity services by faking document, fabricating reports, and lying about the nature and scope of the TSA file found in Denver, it would not have entered into the TSA contracts, renewed the TSA contracts, or paid Tiversa for its claimed funds under the TSA contract.

134. If TSA had known that Tiversa and Boback, on information and belief, provided false statements and fabricated results in its alleged performance of the TSA contract and renewed contract, it would not have paid and/or would have recouped its federal funds from Tiversa, and it would not have renewed its TSA contract.

135. Boback and Tiversa's false representations, false certifications, false reports, lies and critical factual omissions in connection with the TSA contract were misleading and therefore were material misrepresentations.

136. Strict compliance with the specific terms of a federal grant is required. According to the Office of the Inspector General of the United States Department of Justice and the Federal Offices of Inspectors General, "Grant funds are awarded for a specific 'public purpose' and grantees must use those funds as agreed and within certain parameters including the Office of Management and Budget Circulars and granting agency guidelines. . . . A grant agreement is essentially a legally binding contract and grantees are obligated to use their grant funds as outlined in the agreement and to act with integrity when applying for and reporting their actual use of funds." *See Grant Fraud Awareness,* United States Department of Justice, Office of the Inspector General and the Federal Offices of Inspectors General, available at https://oig.justice.gov/hotline/docs/GrantFraudHandout.pdf (last visited on July 27, 2018). Compliance with the terms of the grant go to the essence of the bargain between DHS and Dartmouth, and lack of compliance would have caused the Government not to pay or to recoup some or all of the federal grant funds at issue.

137. Compliance with DHS grant requirements and the grant contracts was a condition of payment for DHS. To ensure compliance, Dartmouth was required to submit quarterly report. DHS retained the right under its grant contract for oversight and to cut off and/or recoup its funds for violations of the terms of the grants. In its quarterly reports, Dartmouth impliedly certified compliance with the law and the terms and conditions of the grants, and by submitting claims for payment, Dartmouth further certified its compliance with the law and the terms and conditions of the grants.

138. Boback and Tiversa's false representations, false certifications, false reports, lies and omissions of critical facts in connection with the DHS grants for Dartmouth in general and the Johnson Paper in particular were misleading and therefore were material misrepresentations.

139. Avoiding and eliminating fraud, waste and abuse in the federal grant process is an important priority to the United States. *Id.*

140. The Government has consistently refused to pay grant recipients and/or pursued grant recipients who violate the terms and conditions of their grants. *See, e.g., United States ex rel. Longhi v. Lithium Power Technologies*, 575 F.3d 458 (5th Cir. 2009) (pursuing technology company for fraudulent scheme to secure research grants from the federal government); *United States ex rel. Resnick v. Weill Medical College of Cornell*, Case No. 04-CIV-3088, 2009 WL 637127, (S.D.N.Y. March 5, 2009) (approving settlement requiring defendant to pay $2.6 million to resolve allegations of FCA allegations that defendant made misrepresentations to obtain Government research grants from DOD and NIH); United *States ex rel. McGee v. IBM Corp.*, 81 F. Supp. 3d 643 (N.D. Ill. 2015) (denying motion to dismiss complaint alleging $50 million in fraud against DHS, among others); *see also* "Yale to Pay $7.6 Million to Settle Grant Investigation," Yale Daily News, Dec. 23, 2008, available at https://yaledailynews.com/blog/2008/12/23/yale-to-pay-7-6-million-to-settle-grant-investigation/ (last visited on July 27, 2018) (settling allegations of fraud in 6000 grants from 30 federal agencies, including DOD, NASA, and DHHS); "Manhattan US Attorney Announces $95 Million Settlement With Columbia University for Improperly Seeking Excessive Cost Recoveries in Connection with Federal Research Grants," Press Release, U.S Attorney for the Southern District of New York, July 14, 2016, available at https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-95-million-settlement-columbia-university-improperly (last visited on July 27, 2018).

COUNT I
False or Fraudulent Claims in Grant Applications,
Grant Program Reports and Grant Research Work Product
(31 U.S.C. 3729(a)(1)(A))

141. Relator incorporates as though fully set forth herein all of the substantive allegations in this Amended Complaint.

142. This is a civil *qui tam* action brought by Relator on behalf of the United States to recover damages, treble damages and civil penalties under 31 U.S.C. § 3729(a) of the FCA.

143. The FCA imposes liability on any person who (A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval (31 U.S.C. § 3729(a)(1)(A)); (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; or (C) conspires to violate either of these two statutory subsections (31 U.S.C. § 3729(a)(1)(C).

144. By virtue of the above-described acts, from 2006 through at least 2009, Boback and Tiversa knowingly caused to be presented false or fraudulent claims for grant payments in the DHS grant application, in DHS grant progress reports submitted to DHS and in the Dartmouth Study funded by the DHS grants.

145. As a result of Defendants' actions and omissions as described more fully herein, they knowingly caused Johnson and Dartmouth to present false or fraudulent claims to obtain grant payments from DHS.

146. These claims were fraudulent for the reasons set forth herein, including the fact that they were (a) based on false, fabricated and/or fraudulent statements regarding compliance with grant terms and research results; and/or (b)included false certifications (express and implied).

147. These false, fabricated and/or fraudulent statements and false certifications were material to DHS's decision to fund the grants.

148. The United States Government has been directly and substantially damaged, and continues to be damaged, as a result of the fraudulent claims and Defendants' conduct in violation of the FCA in an amount to be determined at trial in conformity with the provisions of the FCA

149. The false or fraudulent claims proximately caused additional damages, deprived other researchers of access to scarce federal grant funds and misled other researchers to obtain funds for a study that lacked integrity or value to the Government.

COUNT II
False Records or Statements in Grant Application and Grant Progress Reports
(31 U.S.C. 3729(a)(1)(B))

150. Relator incorporates as though fully set forth herein all of the substantive allegations in this Amended Complaint.

151. This is a civil *qui tam* action brought by Relator on behalf of the United States to recover damages, treble damages and civil penalties under 31 U.S.C. § 3729(a) of the FCA.

152. The FCA imposes liability on any person who (A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval (31 U.S.C. § 3729(a)(1)(A)); (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; or (C) conspires to violate either of these two statutory subsections (31 U.S.C. § 3729(a)(1)(C).

153. As set forth more fully herein, Defendants knowingly made, used, or caused to be made or used, false records or statements material to false or fraudulent claims for grant payments that were made in the DHS grant application, the DHS grant progress reports, the DHS claims for payment by Dartmouth, and grant research work product to DHS, a federal agency funded by the United States Government.

154. The false records or statements are set forth in greater detail herein, but they include (a) false, fabricated and/or fraudulent statements regarding compliance with grant terms and research results; and/or (b) false certifications (express and implied).

155. The false records or statements were material to DHS's decision to award and fund the grants.

156. The United States Government has been directly and substantially damaged, and continues to be damaged, as a result of the false records or statements and Defendants' conduct in violation of the FCA in an amount to be determined at trial in conformity with the provisions of the FCA

157. The false or fraudulent claims proximately caused additional damages, deprived other researchers of access to scarce federal grant funds, and misled other researchers to obtain funds for a study that lacked integrity or value to the Government.

COUNT III
False or Fraudulent Claims in Relating to Tiversa's TSA Contract
(31 U.S.C. 3729(a)(1)(A))

158. Relator incorporates as though fully set forth herein all of the substantive allegations in this Amended Complaint.

159. This is a civil *qui tam* action brought by Relator on behalf of the United States to recover damages, treble damages and civil penalties under 31 U.S.C. § 3729(a) of the FCA.

160. The FCA imposes liability on any person who (A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval (31 U.S.C. § 3729(a)(1)(A)); (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; or (C) conspires to violate either of these two statutory subsections (31 U.S.C. § 3729(a)(1)(C).

161. By virtue of the above-described acts, from 2011 through at least 2013, Boback and Tiversa knowingly caused to be presented, false or fraudulent claims for payment pursuant to Tiversa's contract with the TSA.

162. As a result of Defendants' actions and omissions as described more fully herein, they knowingly, intentionally, and fraudulently induced TSA to enter into and to extend its contract with Tiversa.

163. These claims were fraudulent for the reasons set forth herein, including the fact that they were (a) based on false, fabricated and/or fraudulent statements regarding the scope of the Denver TSA data breach; (b) based upon fabricated false documents knowingly and intentionally created by Tiversa at Boback's direction for the express purpose of lying to TSA about the nature and scope of the alleged data breach and cybersecurity threat; (c) based on false, fabricated and/or fraudulent statements regarding the results of Tiversa's investigating and monitoring under the TSA contract; and/or (d) included false certifications (express and implied).

164. These false, fabricated and/or fraudulent statements and false certifications were material to TSA's decision to enter into the original contract, to execute an additional extension on the contract, and to pay Tiversa for claims it submitted for payment pursuant to the terms of the contract.

165. The United States Government has been directly and substantially damaged, and continues to be damaged, as a result of the fraudulent claims and Defendants' conduct in violation of the FCA in an amount to be determined at trial in conformity with the provisions of the FCA.

COUNT IV
False Records or Statements in TSA Contract with Tiversa
(31 U.S.C. 3729(a)(1)(B))

166. Relator incorporate as though fully set forth herein all of the substantive allegations in this Amended Complaint.

167. This is a civil *qui tam* action brought by Relator on behalf of the United States to recover damages, treble damages and civil penalties under 31 U.S.C. § 3729(a) of the FCA.

168. The FCA imposes liability on any person who (A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval (31 U.S.C. § 3729(a)(1)(A)); (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; or (C) conspires to violate either of these two statutory subsections (31 U.S.C. § 3729(a)(1)(C).

169. As set forth more fully herein, Defendants knowingly made, used, or caused to be made or used, false records or statements material to false or fraudulent claims for payments made pursuant to Tiversa's contract with TSA, a federally funded agency.

170. The false records or statements are set forth in greater detail herein, but they include (a) false, fabricated and/or fraudulent statements regarding the scope of the Denver TSA data breach and the actual cybersecurity risk it posed; (b) fabricated, false documents knowingly and intentionally created by Tiversa at Boback's direction for the express purpose of lying to TSA about the nature and scope of the alleged data breach and cybersecurity threat; (c) false, fabricated and/or fraudulent statements regarding the results of Tiversa's investigating and monitoring under the TSA contract; and/or (d) false certifications (express and implied).

171. These false, fabricated and/or fraudulent statements and false certifications were material to TSA's decision to enter into the original contract with Tiversa, to execute an additional

extension on the contract, and to pay Tiversa claims it submitted for payment pursuant to the terms of the contract

172. The United States Government has been directly and substantially damaged, and continues to be damaged, as a result of the false records or statements and Defendants' conduct in violation of the FCA in an amount to be determined at trial in conformity with the provisions of the FCA.

COUNT V
Conspiracy
(31 U.S.C. 3729(a)(1)(C))

173. Relators incorporates as though fully set forth herein all of the other substantive allegations in this Amended Complaint.

174. This is a civil *qui tam* action brought by relator on behalf of the United States to recover treble damages and civil penalties under 31 U.S.C. § 3729(a) of the FCA.

175. The FCA imposes liability on any person who (A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval (31 U.S.C. § 3729(a)(1)(A)); (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; or (C) conspires to violate either of these two statutory subsections (31 U.S.C. § 3729(a)(1)(C).

176. By virtue of the above-described acts, Boback, Tiversa, and Johnson conspired to violate 31 U.S.C. § 3729(a)(1)(A) and 31 U.S.C. § 3729(a)(1)(B). Specifically, Defendants and Johnson agreed to make false statements material to a false claim to knowingly present or cause to be presented, to officers or employees of the United States, including a member of any agency thereof, these false or fraudulent claims for payment.

177. Defendants and Johnson acted knowingly, as that term is used in the FCA.

178. Unaware of the conspiracy and of the falsity of the records, statements, and claims made or caused to be made by Defendants and Johnson, the United States paid the claims that would not be paid but for Defendants' and Johnson's illegal conduct.

179. Had the United States known of the conspiracy, the false statements, and the false claims that Defendants and Johnson presented or caused to be presented, the United States would not have paid the fraudulent claims.

180. The United States Government has been damaged, and continues to be damaged, as a result of Defendants' conduct in violation of the FCA in an amount to be determined at trial in conformity with the provisions of the FCA.

PRAYER FOR RELIEF

WHEREFORE, Relator requests:

A. That the Court enter judgment against the Defendants in an amount equal to three times the amount of damages the United States Government has sustained because of Defendants' actions, plus a civil penalty of $11,000 for each action in violation of 31 U.S.C. § 3729, and the costs of this action, with interest, including the costs to the United States Government for its expenses related to this action;

B. That Relator be awarded 30% of the proceeds of this action or the settlement of any such claim;

C. That Relator be awarded all costs, attorneys' fees, and litigation expenses; and

D. That the United States Government and Relator receive all relief, both at law and in equity, to which he may reasonably appear entitled.

Dated: July 27, 2018

Respectfully submitted,

JAMES W. HAWKINS, LLC

/s/ *James W. Hawkins*
James W. Hawkins
Admitted *Pro Hac Vice*
Georgia State Bar No. 338767
JAMES W. HAWKINS, LLC
11339 Musette Circle
Alpharetta, GA 30009
V: 678-697-1278
F: 678-540-4515
jhawkins@jameswhawkinsllc.com

Attorney for Plaintiff and Relator
Michael J. Daugherty

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA *ex rel*. Michael J. Daugherty, Plaintiff and Relator, v. TIVERSA HOLDING CORP., TIVERSA INC., TIVERSA GOVERNMENT INC. and ROBERT BOBACK, Defendants.	)	Civil Action No. 14-CV-4548-DLC

CERTIFICATE OF SERVICE

I hereby certify that on July 27, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel for parties of record electronically by CM/ECF.

/s/ *James W. Hawkins*
James W. Hawkins
Admitted *Pro Hac Vice*
Georgia State Bar No. 338767
JAMES W. HAWKINS, LLC
11339 Musette Circle
Alpharetta, GA 30009
V: 678-697-1278
F: 678-540-4515
jhawkins@jameswhawkinsllc.com

Attorney for Plaintiff and Relator
Michael J. Daugherty